NAVEX GLOBAL®

A 12-Step Guide

How to Conduct an Ethics & Compliance Risk Assessment

Contents

INTRODUCTION

Organisations of every shape and size are facing a growing range of ethics and compliance-related risks.

More regulation, rapidly-changing business practices and new working realities are changing organisational risk profiles at an unprecedented pace. As a result, organisations must be able to identify ethics and compliance risks, and respond to them, in order to safeguard their long-term success.

This guide offers a 12-step framework that will help you complete your own ethics and compliance risk assessment. Armed with your findings and action plan, you will be equipped to develop and implement an effective and ethics and compliance programme.

What is an Ethics & Compliance (E&C) Risk Assessment?

An E&C risk assessment can help you understand where unethical or illegal conduct might occur within the organisation. A risk assessment is key to developing your organisation's risk profile. It identifies:

- ethics, compliance and reputational risks your organisation may face given its industry and geography
- risks related to your employee population
- your current and planned mitigation strategies to reduce risk to a level deemed acceptable by your organisation

Defining Ethics & Compliance Risk

For the purposes of this guide, we have defined ethics and compliance risk as a threat posed to an organisation's operational, legal, financial, or reputational standing, resulting from:

- a failure to comply with applicable laws and regulations, and internal standards of ethical conduct, and/or
- unlawful or unethical behaviours of those working for or on its behalf, resulting in legal and reputational damage to the organisation, themselves or others

The approach outlined in this guide can be applied to any form of compliance, ethics, and conduct risk. For instance, it would work equally well for data privacy, bribery and corruption, conflict of interest, financial integrity and fraud, modern slavery and other forms of economic crime.

The broader context

An E&C risk assessment is one element of a broader integrated risk management (IRM) process, and can be conducted concurrently with other risk assessments.

The classic definition of risk management considers risks in relation to their potential negative impact on an organisation's ability to achieve its strategic objectives[1]. It could then be argued that offering a bribe to win a contract may support the strategic objective of generating revenue.

However, bribery can lead to severe fines, prosecution and reputational damage. An effective E&C risk assessment therefore looks beyond the immediate consequences to account for long-term financial and reputational impact.

A well-informed E&C risk assessment looks at:

- the organisation's business model
- the geographic location of its operations
- the industry sector and the competitiveness of the market
- the regulatory landscape
- clients and customers
- products and services
- supply chain and third parties
- transactions and projects
- the ways in which risks may manifest themselves

Don't forget about third parties. NAVEX Global's Definitive Guide to Third-Party Risk Management will help you navigate this increasingly important area of compliance risk. >>>

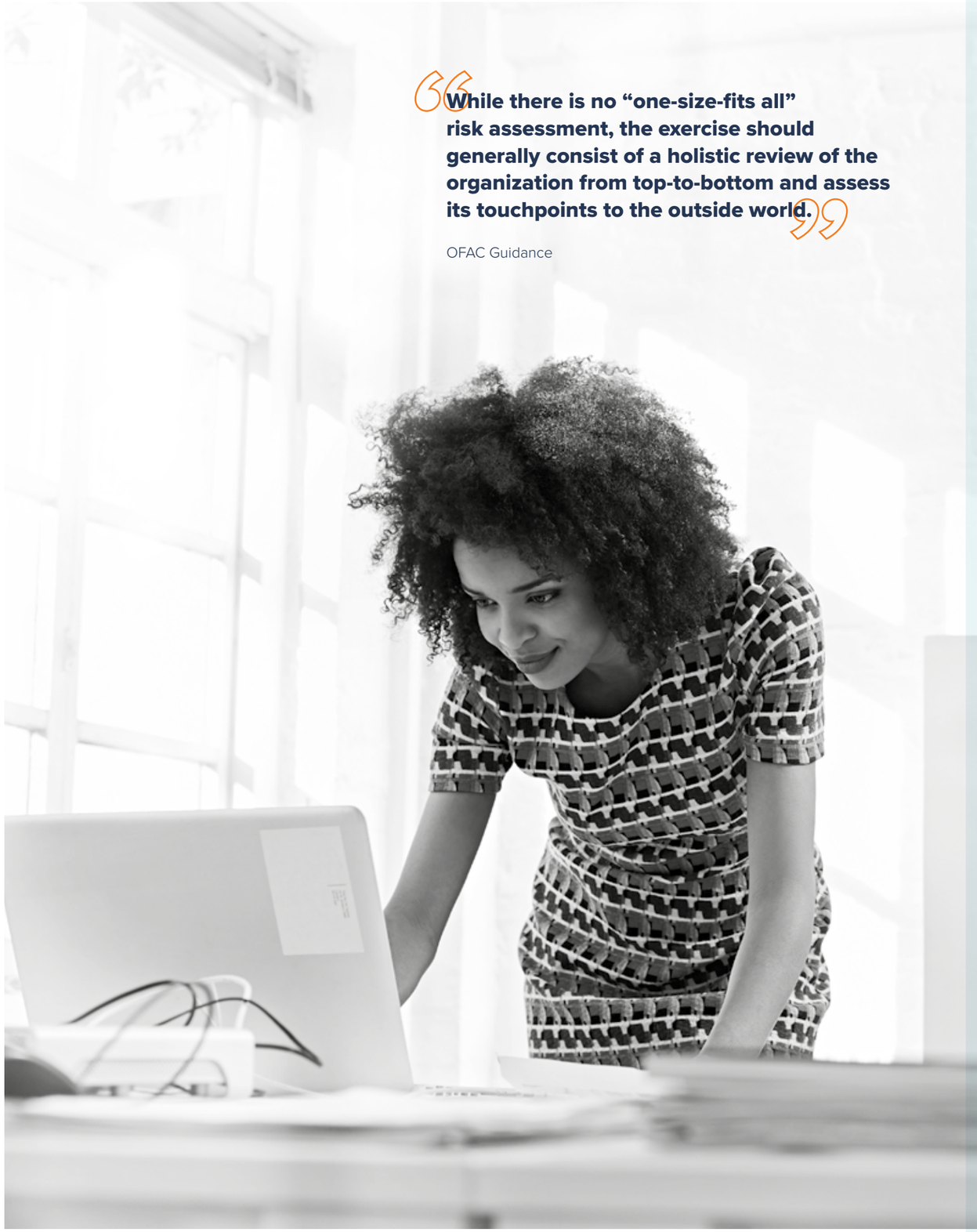
Risk assessment vs Due diligence

While the two terms are often used in relation to each other, there is a difference between risk assessment and due diligence. The latter is a detailed examination of a third party and its financial records, conducted before becoming involved in a business arrangement with it[2]. In that context, a risk assessment will generally inform the extent of the due diligence efforts at various points in a third-party relationship or transaction[3].

[1] COSO Enterprise Risk Management – Integrated Framework, Executive Summary, p. 4 [2] Cambridge Online Dictionary >>> [3] US Department of the Treasury, A Framework for OFAC Compliance Commitments, 2019, p.4

While there is no "one-size-fits all" risk assessment, the exercise should generally consist of a holistic review of the organization from top-to-bottom and assess its touchpoints to the outside world.

OFAC Guidance



Why are Ethics & Compliance Risk Assessments Important?

1 They help you understand your organisation's risk profile

Your risk profile is an evaluation that identifies the unique risks your organisation may face given its industry, geography and employee population. In many cases, organisations may be subject to regulations and vulnerable to risks about which they know little. It can be dangerous to assume you fully understand your organisation's risks. After conducting a thorough risk assessment, you are likely to discover risks that are either new or that have become more significant since the last time you completed an assessment.

According to the *2020 NAVEX Global Definitive Risk & Compliance Benchmark Report*, risk assessment is a high priority ethics and compliance activity with 46% of respondent organisations planning to conduct a comprehensive organisational risk assessment in the next 12 months[4].

2 They provide a strong foundation for your ethics and compliance programme

A proactive, systematic risk assessment is an essential first step to creating and maintaining an effective ethics and compliance programme. Without it the programme may lose credibility because you can't be sure that you have adequate:

- policies, procedures, and controls
- training for the right audiences
- resources invested into the programme
- scrutiny, time and effort allocated to managing and policing risks

In other words, you won't be able to explain why you have chosen to set up the ethics and compliance programme in the way that you have, and why and how your programme has evolved over time[5].

3 They help you meet regulatory expectations

While today's ethics and compliance regulations are numerous, complex, and vary depending on industry and geography, the overarching message remains the same: organisations are expected to adopt a risk-based compliance programme, based on a thoughtful and rigorous assessment of their own risk profile.

Therefore, if your organisation is yet to implement a robust, recurring risk assessment process as part of its ethics and compliance programme, it should become a top priority. Regulators have articulated their expectations for E&C risk assessments in various regulatory guidance. At the same time, they have made it clear that a risk-based approach does not necessarily demand that complex procedures be put in place. For example, a risk assessment for small and medium-sized organisations may comprise a management team brainstorming session that explores potential exposure to ethics and compliance risks.

The key objective of a risk assessment is to identify high-risk areas and focus on those. In other words, organisations are expected to devote a proportionate amount of time, effort and resource to each risk depending on its risk level.

A rigorous E&C risk assessment helps you:

- understand the organisation's exposure to potential criminal, reputational and ethical risks
- design an effective ethics and compliance programme from scratch
- set the agenda or priorities for the compliance activities
- raise awareness of compliance risks with key stakeholders involved in the process
- perform a gap analysis
- enhance procedures and internal controls
- take informed risk management decisions
- measure progress or effectiveness of previous compliance initiatives

Key regulatory requirements for E&C risk assessments

UK Bribery Act 2010	Principle 3 requires that "the commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented."[6]
OECD's 13 Good Practices on Internal Controls, Ethics, and Compliance	According to the OECD guidance, "Effective internal controls, ethics, and compliance programmes [...] should be developed on the basis of a risk assessment addressing the individual circumstances of a company. [...] Such circumstances and risks should be regularly monitored, re-assessed, and adapted as necessary to ensure the continued effectiveness."[7]
U.S. Department of Justice Evaluation of Corporate Compliance Programs	The DOJ's most important guidance document on corporate compliance states that: "The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks."[8]
Sapin II	The anti-corruption programme must include "a risks mapping intended to identify risks according to the business lines and geographical areas where the company carries out business"[9]

[4] NAVEX Global, The Definitive Risk & Compliance Benchmark Report, 2020 [5] US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, p. 2

[6] The Bribery Act 2010 Guidance, p. 25 [7] OECD Council, Good Practice Guidance on Internal Controls, Ethics, and Compliance, adopted 18 February 2010, Annex II, p. 2 [8] US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, p. 2 [9] LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, Chapitre 3, art.17

A Closer Look at COVID-related Business Risks

The coronavirus (COVID-19) pandemic has brought unprecedent challenges, human suffering, major economic disruption and uncertainty on a global scale.

At the same time, its rapid escalation exposed an entire spectrum of ethics and compliance risks such as the vulnerability of supply chains, degradation of public procurement rules, and limitations of existing business continuity plans. These risks are not new, but the pandemic brought their potential magnitude into sharp and immediate focus. A state of urgency, like that seen during the pandemic's onset, create situations and environments ripe for unethical conduct and compliance violations.

NAVEX Global's Coronavirus Comeback Kit will help you identify key back-to-work risks and useful tools and strategies as you plan for the future. >>>

How has the pandemic has changed the risk profile of organisations?

Third party risk
COVID-19 exposed the fragility of supply chains and underscored the crucial role of a robust third-party risk management programme. Unprecedented strain has made it possible for criminals to exploit the situation to defraud companies and government agencies. As a result, the organisational benefits of identifying and managing supply chain risks have become apparent as never before.

Health and safety risks
Re-opening offices and transitioning workforces are likely to exacerbate health and safety concerns and continue to increase liability for organisations. As office workers in many parts of the world return to their workplaces, companies are confronted with a "new normal": the need to ensure compliance with rules on social distancing and personal protective equipment (PPE) use. To ensure a safe return, organisations should conduct "hazard assessments" and implement changes accordingly. Addressing employees' mental health issues including social anxiety and safety concerns is likely to require new support strategies too.

Data security risk
Cyber risks have intensified as more people have moved to work-from-home models. These tend to require the use of unsecure Wi-Fi connections, personal devices, and working environments with a range of listening systems such as smart TVs and speakers. Evidence suggests that the most common and destructive cyber risks occur because employees unknowingly fall prey to cyber threats - that's why changing behaviours through employee training is key.

Behavioural risks
Thanks to the rise in remote working, many of the "normal" workplace practices and daily routines are gone – and with them, the accompanying sense of security. This has increased the potential of behavioural risks among employees, including hot state decision-making, deviations from agreed procedures, and excessive risk-taking. Pressure to perform, increased physical and psychological distance, and less oversight have contributed to an increase in conduct risk.

The COVID-19 pandemic crisis has already forced organisations to revisit their business continuity plans, more thoroughly assess and mitigate supply chain risks and conduct ad-hoc ethics and compliance risk assessments in light of the new behavioral and corruption risks. The job of adapting programmes and practices to meet the challenges will fall to ethics and compliance professionals, working together with risk management, HR, and other groups.

> **"The job of adapting programmes and practices to meet the challenges will fall to ethics and compliance professionals..."**

PLANNING

A high-quality E&C risk assessment requires careful planning.

This section looks at steps 1-6 and explains how to get started with a risk assessment process – from leadership buy-in to stakeholder involvement and automation. No matter how robust your current ethics and compliance programme is, these steps provide a strong foundation for your risk management practice.

Step 1

Get Leadership Buy-in

Active and visible support from senior executives and the board of directors is a key component to secure. Without it, risk assessments can lose momentum, avoid or inadequately deal with certain issues, or have their quality impaired by other executives and managers choosing not to participate.

The board of directors, its equivalent (trustees or advisors), or a designated board committee (including Risk Management Committee or Audit Committee) should have overall responsibility for the risk assessment. They should understand the ethics and compliance risks facing the organisation, drive the risk assessment process and monitor the implementation of risk mitigation activities.

Senior leadership buy-in is key for a successful implementation of a risk response plan. Without their support it may stagnate, as certain functions or individuals may not be willing to give it the importance and attention it deserves. By overseeing the process, the board will be equipped to challenge and energise their management teams.

Tactics to encourage leadership buy-in

Tailor your approach

Become conversant in the company culture, business model, strategic goals and plans to achieve them.

Gear the message around things that matter most to your audience, for example: revenue growth, cost control, staff retention, etc.

Familiarise yourself with the audience's knowledge, values, and preferred communication style.

"Package" the issue

Provide strategic context to your argument and link it to "the big picture".

Provide supporting evidence from industry peers and/or similar companies.

Anticipate questions and issues.

Create a sense of urgency and focus on the benefits.

Bundle with related ideas to give your proposal greater prominence and support.

Establish the communication process

Choose the right timing and communication channel, and be mindful of known, relevant deadlines.

Build a coalition of supporters and allies to accelerate buy-in.

Secure sufficient agenda time and make the most of it.

Manage emotions on both sides: be passionate and seek to inspire positive emotions in decision-makers.

Always follow up afterwards.

Adapted from: SJ Ashford, J Detert, "Get the boss to buy in". Harvard Business Review, 2015 >>>

> **"Senior leadership buy-in is key for a successful implementation of a risk response plan."**

Step 2

Establish the Process

Ask yourself why you're initiating your E&C risk assessment and what results you want to achieve from it (your objectives). Most commonly, this will be to better understand the risk exposure of your organisation so that informed risk management decisions may be taken. Clarity on these points will inform the design of the risk assessment process and should therefore be considered at the planning stage.

The tactics you employ to meet your objectives will vary depending on your organisation's size, business model, its locations, industry and regulatory landscape. Larger organisations may consider centralising or decentralising their risk assessment efforts. Smaller organisations might look to avoid diverting employees away from their daily tasks to ensure there is no disruption to the business.

Defining who should own the risk assessment, and who needs to be involved, is key to the planning stage. A well-planned risk assessment has clearly delineated roles and responsibilities that are communicated and understood. Consider the following points:

The board has overall responsibility for establishing, overseeing, and monitoring the risk assessment process.

Management should be responsible for performing the risk assessment, reporting periodically to the board of directors on the status and results of the risk assessment and on the implementation of the risk mitigation action plans.

Functions that might have responsibility for leading the risk assessment include compliance, legal, ethics, or risk management.

Larger organisations may wish to decentralise risk assessment responsibilities among business units or regions. This may be advisable in situations when the complexity of risks requires specialist or local knowledge.

When should you risk assess?

It makes sense to conduct an E&C risk assessment when your organisation is:

- preparing to implement an ethics and compliance programme
- considering expansion to a new market, sector, country or region
- considering a project or transaction
- facing a regulatory development that might affect the organisation
- contemplating a change in the organisation's business model or business developments like M&A, joint ventures, or greater use of agents or distributors
- evaluating the effectiveness of the existing ethics and compliance programme, its elements and controls

Defining roles and responsibilities in a risk management process

The "Three Lines of Defense" is a risk management model for clarifying roles and responsibilities. It explains the relationship between the functions and serves as a guide to how responsibilities should be divided.

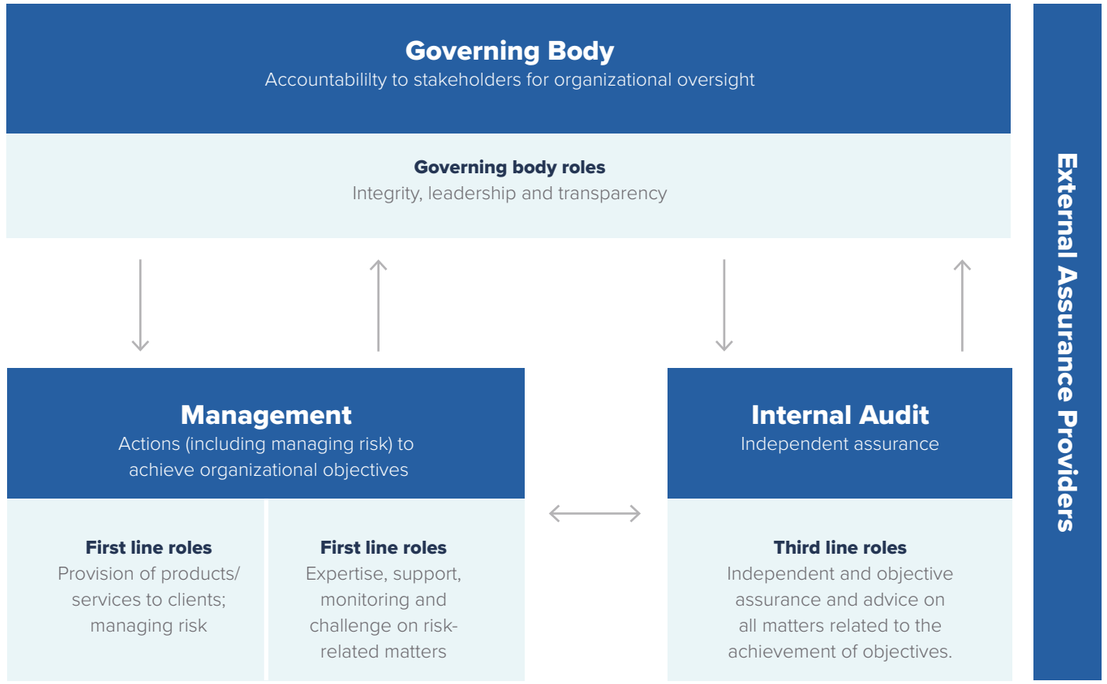
1st Line of Defense – The Doers
The first line of defense is represented by the doers – the people on the front lines. They're managing risk, complying with regulations and standards, and carrying out the company's defined risk management processes daily.

2nd Line of Defense – The Superintendents
The second line of defense is managerial and is responsible for oversight of the doers. They also develop and implement risk management processes, policies and procedures.

3rd Line of Defense – The Investigators
The third line of defense is the auditors, both internal and external, who independently assess and report on the work of the other two lines.

Source: "Three Lines of Defense for Risk Management", 05/08/2020, NAVEX Global >>>

The IIA's Three Lines Model



Source: The Institute of Internal Auditors, "The IIA's Three Lines of Defense Model", 2020, p. 4 >>>

Step 3

Secure Adequate Resources

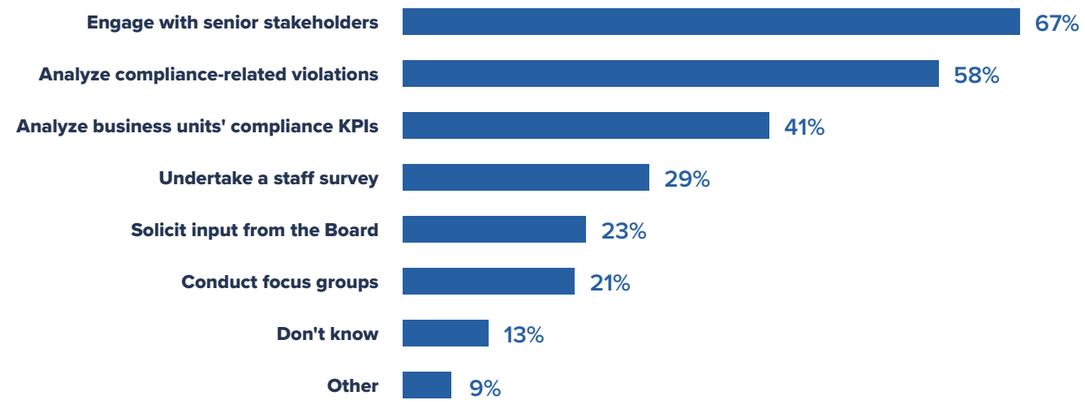
A well-designed E&C risk assessment should include participation and input from many stakeholders - members of senior management, corporate functions personnel, as well as those involved in operations.

The function leading the risk assessment, whether it be compliance or another department, is unlikely to have expertise in every area, and would therefore require support from other functions. These may include legal, risk management, internal audit, sales and marketing, procurement, finance, HR, supply chain and corporate affairs.

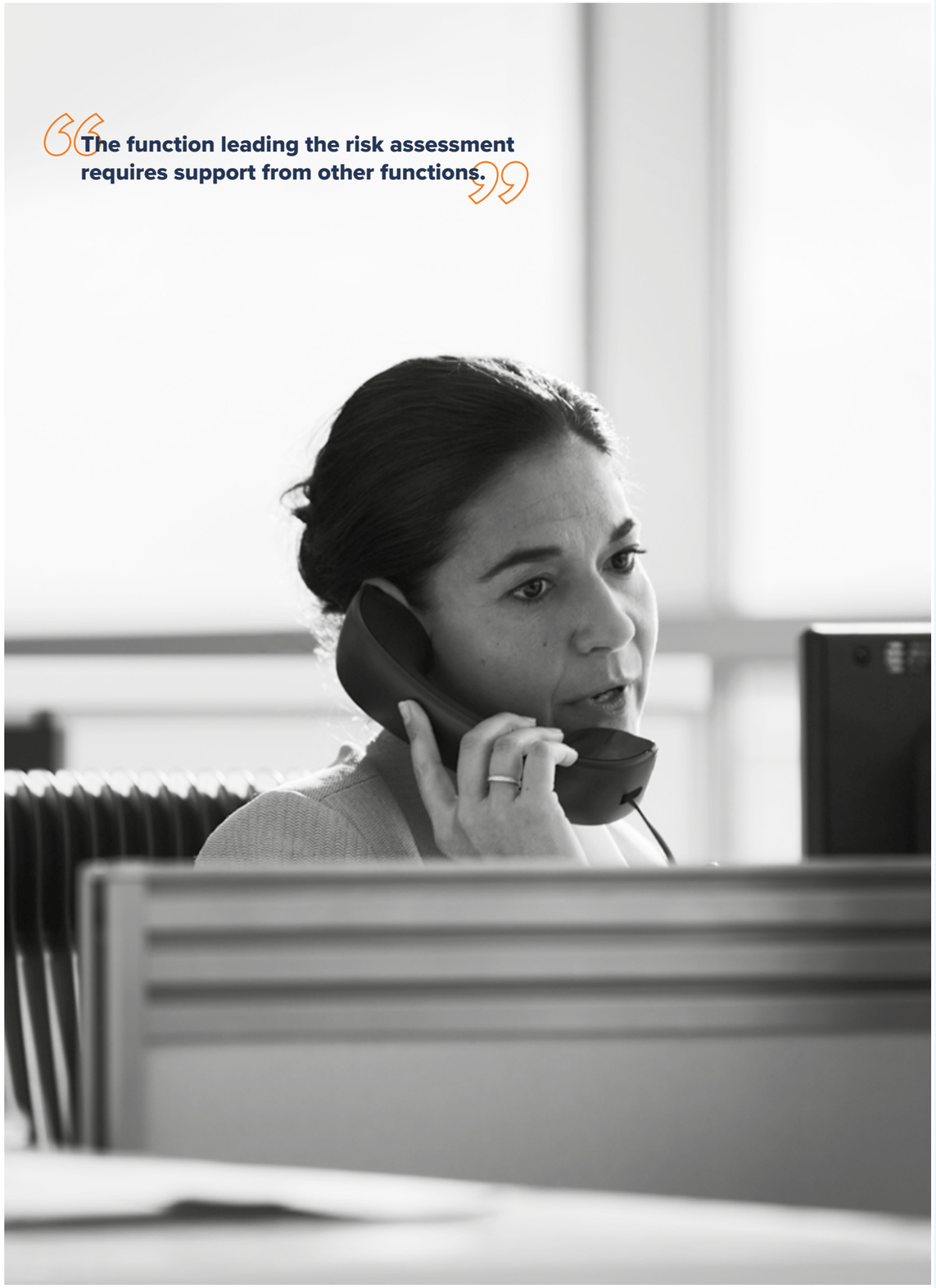
For organisations with a one-person or part-time compliance function, it is advisable to have a committee of individuals/ functions sharing the leadership responsibilities.

Stakeholders should discuss the implementation plan, timeframe, resources and any enhancements that would make the risk assessment more effective. Ensure that each stakeholder has a clearly defined role and a clear understanding of when and how they will be involved. If there is ambiguity about responsibilities, the process could break down or result in unproductive turf battles.

How do you conduct your compliance risk assesment?



Source: PWC State of Compliance Survey 2015 >>>



Step 4

Build a Framework and Methodology

A rigorous E&C risk assessment includes both a comprehensive framework for evaluating and prioritising risk and a methodology to identify, analyse, and address the particular risks it identifies.[10]

The purpose of the framework is to help you integrate risk assessment into the activities, functions, and business processes of your organisation. It allows you to walk through the steps of the process including the identification, assessment, mitigation and ongoing monitoring and reporting of your risks.

The main aim of a risk assessment methodology is to define rules on how the risk assessment should be performed. Rather than practically identifying or assessing risks it states how risks should be identified and assessed, the methods that should be used, the people that should be involved and the documents and templates which are appropriate.

For example, it will state whether the assessment will be qualitative or quantitative. If you don't define this upfront, you may end up with the data that can't be compared (e.g. interview transcripts, historical data, numerical ratings), which may limit the value of your results.

A methodology will also enable you to outline and define specific terms relevant to the risk assessment, including:

- Risk scale
- Internal controls' effectiveness scale
- Risk appetite
- Risk tolerance
- Inherent risk
- Residual risk

Risk management frameworks

ISO 31000: 2018 Risk Management – Guidelines
ISO's framework bases the management of risks on principles, framework, and process. It works well for any type of organisation. ISO 31000 is written for anyone interested in risk management and focuses almost exclusively on risk and incorporating it into the strategic planning process. Many organisations choose to rely on this framework because of familiarity with other ISO standards they are already using.

COSO Enterprise Risk Management – Integrating with Strategy and Performance
Originally issued by COSO in 2004, the framework was revised in 2017 to strengthen the emphasis on the integration of ERM with strategy and performance. The framework is principles-based and focuses on general corporate governance, i.e. how the board should oversee the entire organisation, not necessarily risk. Developed in partnership with one of the "big four" auditing firms, the framework is often considered to be targeted more toward people in the accounting and audit profession.

NIST Risk Management Framework
Developed by the National Institute of Standards and Technology (NIST), which is now part of the US Department of Commerce, the framework outlines the activities related to managing information security risk - today's top risk and compliance concern[11]. It allows companies to determine which systems or applications present the highest risk and implement, assess and monitor security controls. This framework can be combined with NIST Cybersecurity Framework (CSF) to ensure a holistic approach to a broader spectrum of IT-related risks.

NAVEX Global Risk Assessment framework

Use this framework to walk through the steps of a risk assessment process including the identification, assessment, mitigation and ongoing monitoring and reporting of your risks.

1 Identification → 2 Assessment → 3 Mitigation → 4 Monitoring → 5 Reporting

1 Risk Identification
- Create an inventory of the ethics, compliance, legal and reputational risks confronting your organisation, industry and regions
- Assess the likelihood and magnitude of each category or risk and note where there are significant variations by business unit, region and country or employee segment

2 Risk Assessment
- Review and assess organisation-wide processes and efforts to mitigate risks
- Risk rank
- Document mitigation efforts specific to the most important risk areas identified
- Identify gaps in risk management

3 Risk Mitigation & Action Steps
- Assign responsible parties
- Develop action steps and timelines

4 Ongoing Monitoring & Process Repetition
- Monitor risk mitigation
- Regularly repeat the process

5 Reporting & Escalation
- Report assessment results to senior leadership and board
- Share risk assessment with business units
- High level sharing more broadly within the organisation

[10] US Department of the Treasury, A Framework for OFAC Compliance Commitments, 2019, p.5 [11] NAVEX Global, The Definitive Risk & Compliance Benchmark Report, 2020, p.45 >>>

Step 5

Establish your Risk Appetite

Determine the organisation's risk appetite, and risk tolerances, early in the E&C risk assessment process to help streamline the evaluation of residual risk.

If risk appetite is not explicitly determined upfront, there is the potential that management will rationalise existing risk levels as acceptable, undermining the purpose and value of the risk assessment.

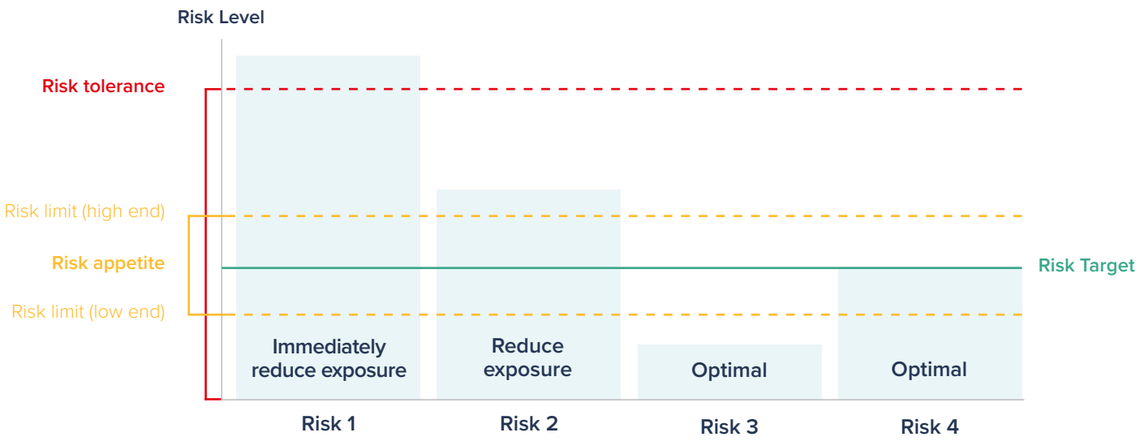
That said, setting a risk appetite is not the same as saying that, for example, a certain amount of bribery is acceptable. The management should always maintain a zero tolerance for corruption. However, it is not sustainable to spend infinite time and resources in managing a risk down to a zero likelihood of occurring, and regulators do not expect you to do so. Instead, you should strive to properly understand a risk and manage it down to a reasonable level.

Note that various documents use the terms 'risk appetite' and 'risk tolerance' interchangeably. However, although related, these are different concepts. Risk appetite is the amount of risk an organisation is willing to pursue or retain and represents a broad view of risk. A risk tolerance is relative to specific risks and performance targets, and can be defined as the organisation's readiness to bear the risk after risk treatment in order to achieve its objectives.[12]

Definitions

Inherent risk	The amount of risk that exists in the absence of controls
Residual risk	The risk remaining after risk treatment
Risk appetite	The amount and type of risk that an organisation is willing to pursue or retain
Risk tolerance	The organisation's readiness to bear the risk, after risk treatment, in order to achieve its objectives

Ethics and compliance risk: Risk tolerance vs Risk appetite



[12] ISO GUIDE 73:2009 Risk management – Vocabulary.

Step 6

Identify Opportunities for Automation

Successful organisations are increasingly adopting technology to automate elements of their compliance and risk management programmes, helping them to reduce costs and increase efficiency.

Following manual processes can increase risk by sustaining a silo-based approach, with individual groups or functions focused on specific risks. Automated governance, risk management and compliance (GRC) platforms, on the other hand, can facilitate a unified approach by: [13]

- Integrating operational, compliance, third party and other risk assessments with appropriate ethics and compliance activities, offering a holistic view of all risk and compliance activities
- Importing and combining relevant data from multiple sources
- Enhancing process maturity by establishing standard, repeatable procedures
- Increasing communication and collaboration between departments and business areas
- Allowing for the development of a unified risk appetite and risk tolerance approach

Looking for an Integrated Risk Management Solution?

The Lockpath platform brings visibility to risks frequently managed in disparate sources including ethics and compliance, business continuity, IT, health & safety and third-party risks. >>>

Common examples of compliance automation

Policy and Procedure Management
An effective system will provide centralised document storage, automatically trigger review or update reminders, and automate policy review and employee attestation tasks based on the rules you've set.

Incident Management Report Routing
Even the most rudimentary incident and case management systems will allow you to set up case workflows and escalation triggers, meaning reports can be automatically routed to the right teams quickly.

Third Party Risk Monitoring and Screening
These systems enable you to screen and continuously monitor your third parties (such as vendors and partners) against risk intelligence databases, and notify you of changes to risk status.

Conflicts of Interest Disclosure Management
Disclosure management tools can help you automate the distribution and notification process for identifying and capturing conflict of interest risks.

Discover how the NAVEX One platform can help you automate your programme. >>>

[13] Lockpath, White Paper '21st century business requires a 21st century compliance and risk management tool', p.2 >>>

IMPLEMENTATION

With clearly defined roles and a strong framework in place, you are ready to begin your risk assessment.

This section covers steps 7-12 and provides tools and templates to identify, assess, and mitigate risks facing your organisation. You will begin by collecting the data to determine risk factors triggering risks.

Step 7

Collect the Data

There are different ways to collect data on how ethics and compliance risks may manifest themselves. Be sure to consider both internal and external resources to create a rounded picture.

Desktop research

Familiarise yourself with the history and current practices of your organisation, employee histories, and organisational culture. Review relevant documents and reports, involve knowledgeable stakeholders and conduct interviews with employees. You may even try to benchmark your operations against similar companies to determine how well you are performing from a regulatory perspective. Internal resources that will give you a head start with your research may include:

- your organisation's criminal records
- past cases of non-compliance and misconduct
- whistleblower hotline reports
- employee background check logs
- internal audit reports on compliance risks
- conflict of interest disclosure forms
- annual HR surveys
- M&A due diligence reports

To determine the industry-specific risks facing your organisation, seek out examples of ethical and regulatory lapses that have been in the news. Take a particular interest in your competitors and peers in this regard and look at the fines and penalties levied against others in the industry.

Reviewing your competitors' Codes of Conduct for hints as to their own perceived risk areas may also give you some perspective. The same approach can be applied to identify country-specific and region-specific risks. Alternatively, consider attending industry webinars and conferences to discuss best practices with fellow compliance professionals.

Interviews

Interviewing key stakeholders can be an effective way to capture an overview of the ethics and compliance risks facing the organisation. Corporate units may offer valuable insights at a high level, while line management (country, regional, or local) may provide additional insights arising from geographic and operational experience. Process owners may be able to identify process-specific issues.

Interviews provide an opportunity to explore specific topics and risks in more detail, although be cautious of confidentiality concerns among interview subjects. Hiring an outside consultant to conduct the interviews is advisable for smaller organisations where anonymity is difficult or impossible to guarantee. If interviewees fear exposure and retaliation for speaking up about risks or wrongdoing of others, they may be reluctant to share the information you're looking for. Consider interviewing the following stakeholders:

- Members of the board of directors
- Suppliers
- Clients
- External auditors
- Investigators
- Local authorities
- Shareholders
- Institutional investors
- Journalists

Benchmarking reports can help you identify the ethics and compliance risks faced by other organisations, and how they are addressing those risks through their own programmes. NAVEX Global's annual risk and compliance benchmark report includes survey responses from over 1,400 professionals globally. >>>

Surveys

Surveys are an efficient way to collect views from both employees and external parties. They can be easy and inexpensive to set up, give respondents the ability to remain anonymous, and enable you to streamline the measurement and interpretation of results through standardised questions. Careful planning and thoughtful structuring is critical to ensure your survey generates meaningful data, rather than new questions or issues.

Organisational culture, and the associated dynamics, can be a risk indicator in itself. An ethical culture assessment survey can help you identify the areas that may be problematic. Evaluating your culture survey results against your whistleblowing hotline data may provide additional insights into the underlying ethical and behavioural risks faced by the organisation.

Self-assessment

A self-assessment is a particularly valuable tool for organisations with different locations and operating units. This is a bottom-up approach where the risk identification is largely driven by the local business' operating environment (rather than developed at corporate level and pushed down to the operating units). However, the data quality may vary. For example, in multinational organisations it's possible that some country managers may think questions on compliance risks from the headquarters will lead to additional controls and reporting lines. This perception may impact their responses.

Workshops and interactive sessions

Using workshops and interactive sessions is another way to collect feedback from different stakeholders. A team of experts may look at individual business processes, map each of them in detail, and then interrogate them to find weak spots. This method may enable participants to not only identify risk indicators, but also propose internal controls to mitigate them.

"Prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners."[14]

DOJ Evaluation of Corporate Compliance Programs

Drive Measurable Value with Your Culture Assessment. Studio Etica's White Paper on Measuring Ethical Culture provides more insight into measuring the key drivers of ethical behaviour. >>>

[14] The US DOJ Criminal Division, 'Evaluation of Corporate Compliance Programs', 2020, p. 3

Step 8

Identify Risk Factors and Risks

Now that you have collected all the relevant data, you should be able to identify ethics and compliance risk factors specific to the nature of your organisation's operations and geographies.

Risk factors are the reasons why risks may occur at the organisation, based on its environment. The analysis of risk factors should be holistic and focus on the entire organisation, including all units, locations, and major accounts.

Once you have a good understanding of risk factors, you can begin to determine what type of underlying risks may exist and how they might manifest themselves, given those factors. You should break the risks down to a reasonable level of detail, keeping in mind that one risk factor can result in multiple risks.

The primary objective of the risk identification is to create a comprehensive inventory of ethics and compliance risks confronting your organisation, industry and regions. It is a critical step to understand what needs to be assessed and what needs to be folded into the overall risk response strategy.

Each risk can take many forms. Take a structured and methodical approach and aim to document all of them in your risk register (see *Step 12: Develop your action plan*).

Example: How a risk factor can exhibit as multiple risks

Risk Factor	Business Climate in Country A		
Risk	**Improper payments to government officials to secure tenders**	**Customs authority requesting a bribe for clearance procedures**	**Sales representatives are offered kickbacks by customers or intermediaries**

Check out NAVEX Global's Seven Crucial Data Privacy Red Flags to discover how you can overcome the risks and turn privacy into a business advantage. >>>

Definitions

Risk factors The reasons why risks may occur at the organisation, based on its environment

Risk register A record of information about identified risks

Residual risk The risk remaining after risk treatment

> **The purpose of a risk assessment is to identify inherent risks in order to inform risk-based decisions and controls.**
>
> OFAC Guidance

Step 9

Rate Inherent Risk

Having identified your ethics and compliance risks, it's time to rate the likelihood that each risk might occur, and the corresponding potential impact of that occurrence. The aim is to prioritise the responses to the identified risks in a logical format.

Assessing likelihood and potential impact can be a subjective process, but the results of your benchmarks, interviews, and other reviews should help you make well-informed decisions. When rating the likelihood, you should disregard the controls already in place. The evaluation of a risk's magnitude should account for financial, operational and reputational damage to the organisation, as well as any negative impacts on employees and other stakeholders.[15] Use a simple three or five-point scoring matrix. On a qualitative scale your classification of likelihood and impact might look like one of the following:

(i) "high", "medium", and "low", or
(ii) "very high", "high", "medium", "low", and "very low".

Alternatively, you could use a quantitative scale with the potential impact and likelihood of a violation weighed from 1-3, or 1-5 respectively. The combination of the likelihood and potential impact assessments gives you the overall inherent risk score for each particular risk.

Human overconfidence and risk assessments

By embracing the insight from the world of behavioural science, you can build a better E&C risk assessment methodology by accounting for the effect of overconfidence.

Overconfidence is a cognitive bias which has often been linked to risky behavior. It reduces risk awareness, leading people to assess risks more optimistically and come to more positive conclusions about anticipated success.

Experiments have shown that an average person has a strong tendency for overconfident judgements when making numerical estimates. Further, when assessing risk, people tend to take into account the probability of a negative event more than the impact of the event.[16]

Take care to account for both effects. Adopt a methodical and evidence-based approach, carefully consider potential negative impacts, and discuss and reconcile your risk perceptions with knowledgeable stakeholders.

[15] Deloitte, Compliance risk assessments The third ingredient in a world-class ethics and compliance program, 2015 >>> [16] Fabricius, G., & Büttgen, M. (2015). Project managers' overconfidence: how is risk reflected in anticipated project success? Business Research, 8, 239-263

Sample rating criteria for rating risk impact (3-point matrix)

Potential Impact	Reputation	Financial	Legal	Employees	Health & Safety	Privacy Infringement	Customers	IT
1 Minor	Local market impact, short term recoverability	<10% of net income	Routine litigations subject to minimal fines and penalties	Isolated instances of employee dissatisfaction and/or above average turnover	Low degree injury or discomfort to an individual or several people	Isolated individual personal detail compromised /revealed	Minor decline in customer relationships, minimal recovery costs	Loss of key systems for less than 1 hour
2 Moderate	Sustained local media attention with escalating implications	10-20% of net income	Routine litigations subject to substantial fines and penalties, regulatory proceedings	Turnover is generally higher than normal, pockets of low morale	Major injury to an individual or several people	Some individual personal details compromised /revealed	Decline in customer relationships, moderate recovery costs	Loss of key systems for 1-5 days
3 Major	National, regional and/or global media coverage, long term damage to the brand and public image	>20% of net income	Significant governing body scrutiny, investigations subject to substantial fines and penalties, criminal charges and proceedings	Loss of leadership team members, decline in employee morale	Death of an individual or several people	All personal details compromised /revealed	Loss of key customers, threat to future growth	Loss of key systems for 5 days or more

How can a risk impact an organisation?

- **Operational impact:** Adverse events, such as embargos or plant shutdowns, that could significantly disrupt the organisation's ability to operate.
- **Financial impact:** Negative impact on the organisation's bottom line, share price, potential future earnings, or loss of investor confidence.
- **Reputational impact:** Damage to the organisation's reputation or brand – for example, bad press or social media discussion.
- **Stakeholder impact:** Negative impacts including loss of customer trust, key personnel leaving the organisation, elevated turnover or decreased employee morale.

Source: Deloitte, Compliance risk assessments The third ingredient in a world-class ethics and compliance program, 2015

Step 10

Identify, Map and Rate Mitigating Controls

Once you have determined the inherent risk, you can begin mapping risks against the internal controls and other risk mitigating activities already in place (for examples, see *Step 12: Develop Your Action Plan*)

This is likely to be a cross-functional, multi-stakeholder effort because many of the controls may be embedded into business processes owned by individual functions.

Start with a review of the process documentation (flowcharts, procedures, written standards and related forms), then supplement this with interviews with relevant stakeholders. Make sure that the controls you catalogue in your risk assessment have been actually implemented (as opposed to only existing "on paper"). When identifying the existing controls, you should also rate their effectiveness in mitigating the risks. To achieve greater accuracy and objectivity:

- base your ratings on the results of independent control testing procedures
- use multiple sources of information
- involve only knowledgeable stakeholders (such as process owners)

A control can be deemed effective when you have confidence, evidence and certainty in its efficacy and can identify the "line of defense" it is covered by.

Use a simple three-point qualitative scale to classify the controls as:

- **Effective**
- **Partially Effective**
- **Ineffective**

Internal controls and how to classify them

Internal controls can be classified in many different ways. For the purposes of the E&C risk assessment, it may be helpful to understand that they can be:

General (organisation-level) vs Risk-specific
General controls are high level and may not be directly related to the risks that you have identified. Nevertheless, they still have a positive impact on risk reduction. Having an ethics and compliance programme, written standards, policies and procedures, compliance training and a whistleblower hotline are all good examples of organisation-level controls.

On the contrary, risk-specific controls will be tightly mapped to the identified risks and will vary from one risk to another.

Preventative vs Detective
Preventative controls are designed to prevent the potential wrongdoing. Examples include a strong ethical culture, written policies, training and communication, and segregation of duties.

The purpose of detective controls is to help detect the misconduct that already took place by performing continuous monitoring, periodic audits, and culture assessments.

Step 11

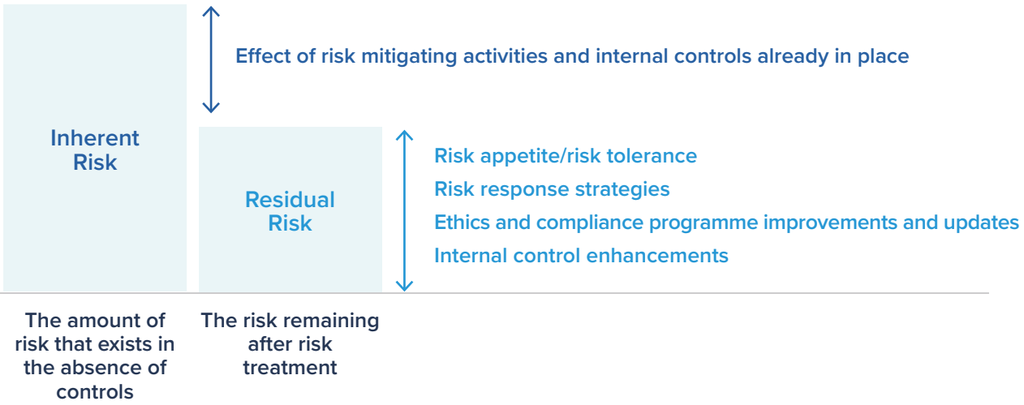
Calculate Residual Risk

Residual risk is the extent of risk remaining after considering the risk-reducing impact of existing controls. The level of residual risk is used to determine whether a risk response is required, and, if so, the right elements of your action plan.

A high residual risk would mean that a high-rated inherent risk is not mitigated by the existing controls in an effective manner, which makes it an area of primary concern for management.

At this point you should also account for your organisation's risk appetite, as no further risk mitigation will be required for a residual risk already within accepted levels.

Residual risk: an illustration



Adapted from: Jason Chorlins and Kaufman Rossin, "Bridging the Gap Between Risk Assessment and Transaction Monitoring", ACAMS Today Magazine, September-November 2017 >>>

> **The level of residual risk is used to determine whether a risk response is required.**

Step 12

Develop Your Action Plan

Once the E&C risk assessment is complete, it's time to draft the action plan that will prioritise your action items. This is a critical step to make sure that necessary enhancements are implemented.

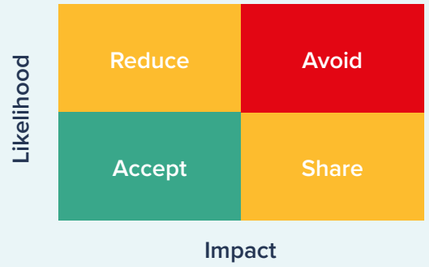
It is important to keep your action plan selective and realistic. Regulators and prosecutors expect organisations to focus on high-risk areas and apply greater scrutiny to them specifically. For example, the DOJ Evaluation of Corporate Compliance Programs guidance states that your ethics and compliance programme is unlikely to qualify as effective if you spend a disproportionate amount of time and resources on policing low-risk areas.[17]

Instead, take a structured, practical approach. Evaluate the need for a response based on the established risk appetite level, and resource constraints, of your organisation. Seek input from functions and individuals who will be responsible for (or impacted by) the action items. Use their input to help you target your efforts to reduce residual risks in an effective and efficient way.

A good action plan should feature the following:

- Identified risk/risk factor
- Description of each action item
- Action owner(s)
- Proposed timeline
- Estimate of resources required to address each action item (e.g. individuals, hours, budget)
- Monitoring and review process: steps required and parties responsible
- Implementation status
- Review date

BEST PRACTICE
Risk response strategies: COSO Methodology[18]



Risk avoidance is a response where you exit the activities that cause the risk. This is because it is deemed difficult or impossible to mitigate the risk in a sufficient and reliable way.

Risk reduction is a response where action is taken to mitigate the risk by enhancing internal controls and/or changing business processes.

Risk sharing (or risk transfer) is a response that aims to reduce the risk by transferring it/its portion to a third party through contract terms.

Risk acceptance is a response where no action is taken because the risk is within the organisation's risk appetite level.

Sample risk register

Risk Factor	Business climate in Country A	Homogeneous workforce in Location B	COVID-19 outbreak	Increase in home working
Risk	Improper payments to government officials to secure tenders	Sexual harassment and improper conduct	Onboarding third parties without proper due diligence to meet crisis-mode tight deadlines	Employee unethical conduct due to uncertainty, stress, anxiety and increased financial pressure
Likelihood	Medium	Medium	High	High
Potential impact	High	Medium	High	High
Inherent risk	High	Medium	High	High
Key mitigating controls	• Code of conduct • Corporate anti-corruption policy including content on payments to government officials • Global whistleblowing hotline • Anti-corruption training programme	• Code of conduct • Corporate anti-discrimination policy including content on sexual harassment • Global whistleblowing hotline	• Standard third-party due diligence process • Onboarding and initial screening against risk intelligence databases • Supplier code of conduct • Audit rights	• Code of conduct • training programmes on code of conduct topics • Global whistleblowing hotline
Control rating/ gaps in controls	Effective	Partially effective	Partially effective	Ineffective
Current residual risk rating	Low	Medium	Medium	High
Target residual risk rating/risk appetite	Low	Low	Low	Low
Management action/ risk response	No action	Develop and roll out anti-discrimination training programme	Implement centralised software system to automate third party screening and monitoring and track any exceptions	Reinforce the organisation's commitment to ethical conduct through awareness materials, manager training, and microlearning courses
Action owner	CCO	HR business partners, CCO, line managers	Head of Procurement, CCO	CCO, HR business partners, line managers
Status	Completed	Open	In progress	Open

[17] US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, p. 3 [18] COSO Enterprise Risk Management – Integrating with Strategy and Performance (2017)

MEASURE

An effective E&C risk assessment is dynamic and should evolve alongside your ethics and compliance programme and your organisation.

You should continually evaluate whether your risk assessment efforts are in alignment with the organisation's internal developments and external environment. Monitor your progress and be sure to repeat and update your risk assessment at least annually.

Monitor, Measure and Improve

The importance of implementing the action plan cannot be overstated. Regulators and prosecutors expect you to update your policies, procedures, and controls in light of lessons learned from your periodic risk assessments. These updates should account for the risks you've identified.

Although you will have many stakeholders from various functions responsible for the implementation of action items, it is important to nominate one individual who will coordinate the efforts and provide progress reports to the board and senior management. The monitoring of risk mitigation should be performed on a continuous basis, with any necessary amendments made and approved by the board in a timely manner.

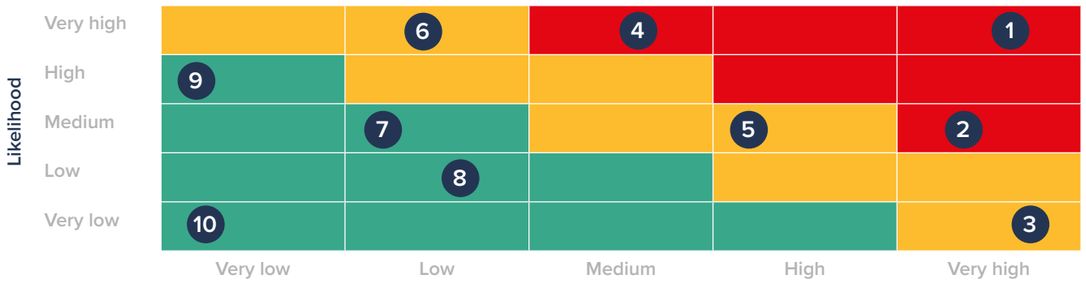
To drive discipline in the implementation process, consider linking the successful delivery of action items with individuals' and functions' goals and performance evaluations.

Definitions

Inherent risk The amount of risk that exists in the absence of controls

Control risk The chance that an ethics and compliance risk would materialise because of a failure in an organisation's system of internal controls

Simple risk assessment matrix or 'heat map'[19]



Key

X Risk

The organization conducts…[…] a risk assessment in a manner, and with a frequency, that adequately accounts for the potential risks.[20]

OFAC Guidance

[19] Adapted from: UNGC, A Guide for Anti-Corruption Risk Assessment, 2013, p.71 [20] US Department of the Treasury, A Framework for OFAC Compliance Commitments, 2019, p.4

Report and escalate

Compile all of your findings, recommendations, and action items in a comprehensive report. This report can be shared with business units and those functions/individuals who will need to see this level of detail. The board and senior management are likely to benefit from a concise summary of the key risks identified, key control gaps, and the action items planned to address the risks in order of priority.

A risk "heat map" is an impactful way to present the results of your risk assessment to the board. Simple heat maps typically have sections that are red (high risk), yellow (medium risk) or green (low risk). A more detailed heat map would have inherent risk ratings on one axis and control risk ratings on the other. This approach visualises the interplay between inherent risk and control risk, giving a clear picture of the effectiveness of risk mitigating controls against the identified risks. It also helps to overcome the bias of focusing only on high-impact, high-likelihood risks. As we have learned from the COVID pandemic, high-impact and low-likelihood risks require treatment, too.

Your summary report should include:

- Statement of objectives
- Assessment scope
- Locations and business units covered
- Established risk appetite and risk tolerance levels
- Key procedures/work steps
- Key stakeholders
- Key risk areas
- Key controls
- Key action items from the response plan
- Key statistics
- Data visualisation (e.g. graphs and charts)

NAVEX Global's Definitive Guide to Ethics & Compliance Programmes provides actionable guidance on how to design and implement a robust programme. >>>

Done? Now repeat

It is best practice to complete an E&C risk assessment regularly (at least annually), not just when developing or refreshing your ethics and compliance programme.

This is likely to be an optimal timeframe because enforcement trends, such as those involving anti-corruption, trade, antitrust, data privacy and anti-money laundering laws, evolve rapidly. At the same time, organisations (particularly large or multinational companies) tend to go through numerous significant changes within a given fiscal year.

You should also be open to completing a new risk assessment on an "as needed" basis, such as when marketing a new product, or entering into a new business venture.

According to the *2020 NAVEX Global Definitive Risk & Compliance Benchmark Report*, 66% of organisations perform a periodic risk profile assessment, and this percentage increases with programme maturity level (99% in organisations with "Advanced" risk and compliance programmes).[21]

Build the annual risk assessment into your ethics and compliance programme and try to complete it at the same time each year. It will be helpful to demonstrate to regulators, shareholders and other key external stakeholders that your risk assessment is a formal corporate process rather than an occasional, ad-hoc exercise.

Update and improve

Your risk assessment should not be a "snapshot" in time Prosecutors expect you to have a process for tracking and incorporating lessons learned into periodic risk assessments. Your updates and revisions should therefore reflect the following risk indicators:[22]

- Cases of misconduct and other issues/problems linked to the ethics and compliance programme encountered by your organisation
- Compliance/regulatory issues encountered by other organisations in your industry/ geographical region

These, along with audit findings, internal controls testing results, and root cause analysis of any apparent violations or identified systemic deficiencies, should inform your risk assessment. In turn, this should result in appropriate updates to policies, procedures and controls, keeping your ethics and compliance programme risk-tailored and up to date.

[21] NAVEX Global, The Definitive Risk & Compliance Benchmark Report, 2020, p.42 >>> [22] US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, p.4

About the Author

Vera Cherepanova
Ethics Advocate, Consultant, Author
Studio Etica, Milan (Italy) ›››

Vera Cherepanova is a former Regional Compliance Officer and author of “Compliance Program of an Organisation.” Vera has worked on the ground in Eastern Europe, CIS and Russia. Taking her experience in addressing the cross-cultural challenges of ethics and compliance, Vera currently consults with international corporations, non-profits, wholesale and retail establishments, and small to large businesses, advising them on ethics and compliance programmes. Vera speaks Russian, English, French, and Italian.

About NAVEX Global® Solutions

NAVEX Global is the worldwide leader in integrated risk and compliance management software and services.

Our solutions are trusted by thousands of customers around the globe to help them manage risk, address complex regulatory requirements, build corporate ESG programmes and foster ethical workplace cultures. For more information, visit **www.navexglobal.com**

NAVEX One® Ethics and Compliance Platform

The integrated NAVEX One® platform offers risk, compliance, legal and HR professionals a unified view and streamlined workflows across multiple applications, making it easier to manage and administer ethics and compliance programmes.

Give your employees access via single sign-on to a unified view into their compliance tasks related to policies, training and disclosures, and ease the compliance burden on both administrators and employees to improve your organisation’s compliance with corporate, legal and regulatory requirements.

Consolidate your entire ethics and compliance program onto a scalable cloud-based platform, enabling you to confidently anticipate and navigate global regulatory compliance.

Watch the video

An Integrated Platform to help you effectively manage your Ethics and Compliance Program.

NAVEX One® Ethics & Compliance Platform
›››

Appendix

Key Definitions
ISO/Guide 73:2009 Risk management – Vocabulary

Control
Measure that is modifying risk

Inherent risk
The amount of risk that exists in the absence of controls

Residual risk
Risk remaining after risk treatment

Risk
Effect of uncertainty on objectives

Risk appetite
Amount and type of risk that an organisation is willing to pursue or retain

Risk assessment
Overall process of risk identification risk analysis and risk evaluation

Risk criteria
Terms of reference against which the significance of a risk is evaluated

Risk impact (or consequence)
The cost of a risk if it does occur

Risk likelihood (or magnitude)
The probability that risk will materialise

Risk management
Coordinated activities to direct and control an organisation with regard to risk

Risk management framework
Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation

Risk management process
Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk

Risk matrix
Tool for ranking and displaying risks by defining ranges for likelihood and impact

Risk tolerance
Organisation's readiness to bear the risk after risk treatment in order to achieve its objectives

Risk register
Record of information about identified risks

Risk treatment
Process to modify risk

Additional Resources

Risk Assessment Frameworks

COSO Enterprise Risk Management – Integrated Framework ›››
COSO "Risk Appetite – Critical to Success. Using risk appetite to thrive in a changing world" ›››
ISO 31000:2018 Risk Management – Guidelines ›››
ISO GUIDE 73:2009 Risk management – Vocabulary ›››
NIST Risk Management Framework ›››
The IIA's Three Lines of Defense Model 2020 ›››
UNGC, A Guide for Anti-Corruption Risk Assessment ›››

NAVEX Global® Resources

Coronavirus Comeback Kit ›››
Corruption Risk Country Profiles ›››
Definitive Guide to Compliance Programme Assessment ›››
Definitive Guide to Ethics & Compliance Training ›››
Definitive Guide to Policy and Procedure Management ›››
Definitive Guide to Third-Party Risk Management ›››
Definitive Guide to Whistleblowing Hotlines ›››
Definitive Guide to Your Code of Conduct ›››
Ethics & Compliance Third Party Risk Management Benchmark Report 2016 ›››
Risk Assessment Framework ›››
Sample Risk Prioritization Framework ›››
Sapin II Legal Brief ›››
Seven Crucial Data Privacy Red Flags ›››
The Definitive Corporate Compliance Benchmark Report 2019 ›››
The Definitive Risk & Compliance Benchmark 2020 ›››
White Paper: "21st century business requires a 21st century compliance and risk management tool" ›››
White Paper: Anti-Bribery and Corruption Risk Assessment Checklist ›››
White Paper: "Bribery and Corruption Red Flags "How to Respond to Corruption Indicators" ›››

Studio Etica Resources

White Paper Measuring Ethical Culture ›››

International Guidance on E&C risk assessments

2018 Federal Sentencing Guidelines Manual ›››
A Framework for OFAC Compliance Commitments ›››
OECD Good Practice Guidance on Internal Controls, Ethics, and Compliance ›››
UK Anti-Bribery Act Guidance from Transparency International ›››
U.S. Department of Justice Evaluation of Corporate Compliance Programs ›››

EMEA + APAC

Vantage London – 4th Floor
Great West Road, Brentford TW8 9AG, UK

www.navexglobal.com
+44 (0)20 8939 1650

Americas

5500 Meadows Road, Suite 500
Lake Oswego, OR 97035, USA

www.navexglobal.com
+1 (866) 297 0224

PLEASE RECYCLE

NAVEX GLOBAL®